

Michael Brückner / Andrea Przyklenk

Kursbuch Datenschutz

Der Ratgeber gegen den Röntgenblick

LESEPROBE

Haben Sie Fragen an die Autoren?

Anregungen zum Buch?

Erfahrungen, die Sie mit anderen teilen möchten?

Nutzen Sie unser Diskussionsforum:

www.mankau-verlag.de

mankau

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Michael Brückner / Andrea Przyklenk

Kursbuch Datenschutz

Der Ratgeber gegen den Röntgenblick

ISBN 978-3-938396-33-9

1. Auflage 2009

Mankau Verlag

Postfach 13 22, D-82413 Murnau a. Staffelsee

Im Netz: www.mankau-verlag.de

Diskussionsforum: www.mankau-verlag.de/forum.php

Lektorat / Endkorrektorat: Dr. Thomas Wolf, MetaLexis

Gestaltung Umschlag: Guter Punkt, München,

Andrea Barth | www.guter-punkt.de

Gestaltung Innenteil: Heike Brückner, Grafikstudio, Regensburg

Hinweis des Verlags

Die Autoren haben bei der Erstellung dieses Buches Informationen und Ratschläge mit Sorgfalt recherchiert und geprüft, dennoch erfolgen alle Angaben ohne Gewähr; Verlag und Autoren können keinerlei Haftung für etwaige Schäden oder Nachteile übernehmen, die sich aus der praktischen Umsetzung der in diesem Buch dargestellten Inhalte ergeben.

Der Inhalt wurde auf chlorfrei gebleichtem Recyclingpapier gedruckt, der Druck erfolgte in Deutschland.

Inhalt

Vorwort.....	9
I. Big Brother kommt auf Samtpfoten	13
Erfolgreiche Terrorbekämpfung oder Einstieg in den Überwachungsstaat?.....	13
Im Raster der Kontroll-Freaks.....	24
Der müde Widerstand der Bürger	31
II. Der unstillbare Datenhunger des Staates	45
Der „denkbar größte staatliche Eingriff“	45
Alles auf eine Karte: die neuen Pässe und Ausweise	65
Big Fiskus is watching you: die Kontrollwut der Finanzbehörden	75
III. Halali auf den Verbraucher	105
Die geheimen Tricks der „Numerati“	105
Rabattsysteme als Trojanische Pferde	112
Mobil, mobiler, Handy: Datenfang mit dem Schleppnetz.....	123
Gewinnspiele – für dumm verkauft	129
Was eBay & Co. über uns verraten	133
Customer Relationship Management – Tante Emma ade!.....	138
Datenhandel – ein Zukunftsmarkt.....	143
IV. Der Röntgenblick von Banken & Co.	149
Das verräterische Girokonto	149
Kundendaten als Rohstoffe für gezieltes Cross-Selling	153

Interne Wächter: die Geldwäschebeauftragten der Banken und Versicherungen	155
SWIFT: die CIA liest mit	159
Scoring-Verfahren: Risiko-Management oder Finanz-Esoterik?	163
Die Schufa: Datenmonster oder vertrauensfördernde Organisation?.....	167
Uniwagnis: die Frühwarn-Datei der Versicherer.....	172
V. Der freiwillige Daten-Exhibitionismus.....	177
Internet – Infoquelle und Schrotthalde	177
Web 2.0 und die Lust am privaten Daten-Striptease	179
Die besondere Risiken sozialer Netzwerke	186
Communitys – das Zuhause in der virtuellen Welt.....	192
Gefährliche Chatrooms	197
Wenn das Internet zur Karrierefalle wird	203
Das verräterische Handy.....	209
VI. Datenschutz in Europa.....	213
Exoten entern die politische Bühne.....	213
Schweiz: die Bedenken der Eidgenossen.....	217
Österreich: Rückschlag beim Datenschutz.....	222
Die Europäische Datenschutzrichtlinie	226
Sonderteil: Kinder und Jugendliche im Netz.....	231
Risiko! Wenn Kinder surfen	231
Was Ihre Kinder im Netz treiben	235
Virtuelle Gefahren für Ihr Kind	240
Nutzen im Netz	260
Tipps für Eltern.....	262

Datenschutz von A bis Z: Kleines Glossar.....	269
Die wichtigsten Web-Links von A bis Z	281
Weiterführende Literatur.....	283
Zu den Autoren.....	285

Vorwort

Es war eine E-Mail von höchster Brisanz, die Ende 2007 die Redaktion des Hamburger Magazins „stern“ erreichte. Und den Journalisten, die diese mutmaßliche Insider-Botschaft lasen, war sofort klar: Wenn die darin enthaltenen Behauptungen tatsächlich zutreffen sollten, dann drohte der Republik ein Datenskandal ungeahnten Ausmaßes. Im Zentrum der Vorwürfe stand eines der führenden deutschen Handelsunternehmen. Der E-Mail-Verfasser schrieb der Redaktion, ihm lägen Protokolle vor, mit denen sich die systematische Überwachung von Mitarbeitern eines führenden Lebensmitteldiscounters beweisen lasse. Nun sind E-Mails, in denen die Absender schwere Vorwürfe gegen Unternehmen, Politiker, Behörden oder sonstige Institutionen erheben, nicht eben selten, und es gehört zu den besonderen journalistischen Herausforderungen, Hinweise auf tatsächliche Skandale von haltlosen Beschuldigungen und Verdächtigungen zu unterscheiden. Im konkreten Fall jedenfalls witterten die Redakteure Malte Arnsperger und Markus Grill eine Geschichte. Sie trafen den Informanten, fühlten ihm auf den Zahn, um seine Glaubwürdigkeit zu testen, und sichteteten anschließend mehr als 500 Seiten Material, das der Insider ihnen überreichte. Die Journalisten recherchierten minutiös die Zusammenhänge und erkannten bald, dass sie einer wirklich haarsträubenden Affäre auf der Spur waren. Schließlich konfrontierten sie das Unternehmen mit den Vorwürfen – und dort läuteten plötzlich alle Alarmglocken. Ein PR-Desaster ersten Ranges zeichnete sich ab.

Etwa drei Monate, nachdem sich der Informant mit seiner E-Mail an „stern.de“ gewandt hatte, veröffentlichte das Magazin im März 2008 eine Titelgeschichte über die Bespitzelungsaffäre beim Lebensmitteldiscounter Lidl. Der Skandal sorgte bundesweit für Schlagzeilen und Empörung. Die Autoren der Enthül-

lungsstory wurden vom „Medium Magazin“ als „Journalisten des Jahres“ ausgezeichnet. Lidl hingegen musste ein Bußgeld von knapp 1,5 Millionen Euro zahlen. Nachdem schließlich im April 2009 bekannt wurde, dass der Discounter Krankheitsdaten seiner Mitarbeiter sammelte, reagierte das Unternehmen mit der Entlassung seines Deutschland-Chefs.

Dabei schien die Lidl-Affäre nur die Spitze des Eisbergs zu sein. Immer neue gravierende Verstöße großer deutscher Unternehmen kamen nun ans Tageslicht. Zu den spektakulärsten Fällen gehörte sicher der Daten-Skandal bei der Deutschen Telekom und der Deutschen Bahn. Beinahe täglich neue, spektakuläre Enthüllungen ramponierten das Image beider Unternehmen.

Aber auch der Staat geht nicht eben zimperlich mit den persönlichen Daten seiner Bürger um. Von der Vorratsdatenspeicherung über das BKA-Gesetz bis hin zur automatisierten Kontenabfrage durch Finanzämter und Sozialbehörden reicht die Liste von fragwürdigen Überwachungs- und Kontrollmethoden der Behörden. „Wenn man alles zusammennimmt, was jetzt erlaubt werden soll, hätte man das vor zehn Jahren für unmöglich gehalten“, stellt der Staatsrechtsprofessor und ehemalige Verfassungsrichter Dieter Grimm erstaunt fest.

So skandalös die Datenskandale der vergangenen Monate und Jahre auch gewesen sein mögen, letztlich trugen sie doch dazu bei, die Sensibilität der Bürger für den Datenschutz wieder zu erhöhen. Im Zuge der Bekämpfung von Terror, Geldwäsche und Steuerhinterziehung schossen die Politiker in den vergangenen Jahren nicht selten über das Ziel hinaus und stellten kaum noch die Frage nach der Verhältnismäßigkeit der Mittel. Und auch die Bürger nahmen Einschränkungen ihrer informationellen Selbstbestimmung und zunehmende Überwachung (wer stört sich heutzutage noch an den zahlreichen Videokameras in den

Innenstädten?) mit bemerkenswertem Gleichmut hin. Welch ein Unterschied gegenüber den Protesten gegen die Volkszählung in den 1980er Jahren. Einerseits erscheint dieses mangelnde Interesse an effektivem Schutz der persönlichen Daten äußerst bemerkenswert, haben doch die Fortschritte der Informationstechnologie in den zurückliegenden zwanzig Jahren die Risiken eines potenziellen Datenmissbrauchs drastisch erhöht. Andererseits kann das lange Zeit mangelnde Engagement der Bundesbürger für Privacy und den Schutz ihrer Daten kaum überraschen. Denn während die Politik hehre Gründe für ihre Überwachungsmaßnahmen ins Feld führt (wer könnte schon gegen die Terrorismusbekämpfung sein?), leben wir gleichzeitig in einer Welt der Selbstdarstellung. Es ist erstaunlich, was manche Bürger freiwillig an persönlichen Daten, Ansichten und Vorlieben im Internet preisgeben. Ausgerechnet in einem Medium, dessen elektronisches Gedächtnis nie etwas vergisst. So mancher Bewerber machte daher schon große Augen, wenn er im Interview bei seinem neuen Arbeitgeber mit einer Jugendsünde konfrontiert wurde, von der er selbst locker im Internet berichtet hatte.

Wie gesagt, die Datenskandale der jüngeren Vergangenheit trugen dazu bei, manches wieder etwas kritischer zu sehen. Dazu gehört auch die Frage, ob man für ein paar Rabattpunkte beim Händler freiwillig seine persönlichen Daten und Konsumgewohnheiten publik machen sollte. Um es gleich vorwegzunehmen: Die Autoren des vorliegenden Buches meinen „nein“.

Auf den folgenden Seiten erfahren Sie, wo die Daten-Fallen im Alltag lauern – vom Internet bis hin zu „Big Fiskus“. Gleichzeitig geben wir Ihnen konkrete Tipps, wie Sie Ihre Privatsphäre bestmöglich schützen können. Denn denken Sie immer daran: Wissen ist Macht. Je mehr ein Unternehmen oder eine Behörde über Sie weiß, desto größer ist die Macht, die über Sie ausgeübt werden kann. Jeder Mensch hat ein Recht auf optimalen Schutz

seiner persönlichen Daten, die Wahrung seiner Privatsphäre und auf seine ganz individuellen Geheimnisse. Davon sind die Autoren überzeugt. Und deshalb ist das vorliegende Buch nicht nur eine Bestandsaufnahme und ein Ratgeber, sondern auch ein Plädoyer:

Diskretion statt Datengier!

Ingelheim/Leonberg, im September 2009
Michael Brückner & Andrea Przyklenk

I. Big Brother kommt auf Samtpfoten

Erfolgreiche Terrorbekämpfung oder Einstieg in den Überwachungsstaat?

Erinnern Sie sich noch an die Volkszählung Anfang der 1980er Jahre? Was war das damals für ein Aufstand. Die Angst vor dem Überwachungsstaat trieb Hunderttausende von Bundesbürgern um. Zeitweise gab es über 1.000 Bürgerinitiativen gegen die Volkszählung. Sie protestierten auf Demonstrationen oder beschritten den Rechtsweg. Am 13. April 1983 entschied der Erste Senat des Bundesverfassungsgerichts, dass die Volkszählung in der geplanten Form nicht durchgeführt werden könne. Die Richter fanden die Anonymität der Bürger nicht ausreichend gesichert. Außerdem bemängelten sie den geplanten Vergleich zwischen den Angaben in den Fragebögen und den Daten in den Registern von Standesamt und Arbeitsamt. Letztlich dauerte es bis 1987, um die Volksbefragung juristisch auf festen Boden zu stellen.

Und heute? Digitaler Ausweis, Austausch von Flugdaten mit den USA, Schnüffelaffären in unüberschaubarem Ausmaß in den Unternehmen, von den Möglichkeiten, die IT, Internet und Telefon heute bieten, ganz zu schweigen. Trotzdem flammt kaum ernst zu nehmender Widerstand auf. Haben wir angesichts der technischen Möglichkeiten der Sammler und Schnüfler aufgegeben oder ist uns die Terrorbekämpfung wichtiger als der Schutz unserer eigenen Daten? Hat am Ende der Datenschutz nicht mehr die gleiche Priorität wie früher? Wenn man sich anschaut, was in Internetforen und Blogs, in Chats, auf YouTube und MySpace ins weltweite Netz gestellt wird, scheint diese Annahme zumin-

dest nicht ganz abwegig. Die Gesellschaft des 21. Jahrhunderts ist freier, offener und exhibitionistischer geworden. Der Staat, die Unternehmen und zwielichtige Geschäftemacher nutzen diese Schwäche aus. Ihre Möglichkeiten sind nahezu unendlich – dafür sorgt die sich schnell entwickelnde Informationstechnik. Seit den Zeiten des Widerstands gegen die Volkszählung, als das Bundeskriminalamt seine Daten noch in schrankgroßen Computern sammelte, die nicht einmal über einen Bruchteil der Schnelligkeit und Fähigkeiten heutiger Systeme verfügten, hat die Technik einen Quantensprung gemacht. Das Internet war damals außer bei einigen Wissenschaftlern noch gar kein Thema. Von Handys redete kein Mensch.

Schweinefleisch und Alkohol

Gleich vorneweg: Wir glauben, dass man sich vor der Datensammelwut staatlicher Stellen noch weniger wirksam schützen kann als vor der privater Unternehmen. Dafür hat der Staat selbst gesorgt. Unter dem Deckmantel des Servicegedankens können wir heute nahezu alle Geschäfte, zu denen wir uns früher ins Rathaus oder andere Ämter begeben mussten, über den PC abwickeln: Steuererklärungen, Autos anmelden, Wahlunterlagen beantragen usw. Auch die staatlichen Stellen wickeln vom Kindergeld über das Arbeitslosengeld und Hartz IV alles über die EDV ab. Das heißt, unsere Daten liegen sowieso elektronisch vor und im Ernstfall können wir sogar über die IP-Adresse unseres Computers identifiziert werden.

Wir amüsieren uns bisweilen über die amerikanischen Fernsehfilme oder -serien, in denen superschlaue Ermittler ruck, zuck alles über einen Verdächtigen wissen oder der Geheimdienst eine Identität via PC völlig auslöschen kann. Vielleicht sollten wir nicht darüber lachen, sondern davon ausgehen, dass

das keine Zukunftsmusik ist, sondern bereits Realität. Natürlich verhindern Gesetze, dass jemand ohne Verdacht auf unsere Daten zugreift, aber was heißt das schon? Schließlich sind es Menschen, die Zugriff zu unseren Daten wollen und haben. Weshalb sollten sie die Vorschriften nicht übertreten? Wieso sollte es bei den Geheimdiensten keine Verschwörungen zur Umgehung der Vorschriften geben oder einfach Pannen? Halten Sie die Politik wirklich für fähig, Geheimdienste und Polizei zu kontrollieren?

Das alles mag nicht schlimm erscheinen, wenn man ein reines Gewissen und nichts zu verbergen hat. Doch die deutsche Geschichte hat gezeigt, was deutsche Staaten vermochten, die nicht einmal über Computer und Datenautobahnen verfügten. Gestapo und Stasi hätten Freudentänze vollführt, wenn sie unser heutiges Instrumentarium zur Überwachung des Volkes in der Hand gehabt hätten. Letztlich landen wir damit bei der Frage, wie weit und ob wir unserem Staat vertrauen. Und nicht nur das: Wir landen auch bei der Frage, ob wir durch Überwachung und Bespitzelung ein Klima schaffen können, in dem Terrorismus nicht gedeiht. Die Antwort ist: Jede Gewalt gedeiht in einem Klima der Angst und des Misstrauens am besten. Und darunter leiden bei uns seit den Terrorismusbekämpfungspaketen besonders die Ausländer. Wenn sie dann noch Moslems sind, geraten sie rasant schnell ins Visier der Fahnder. Denn man sucht ja nicht nach solchen, die auffallen, sondern nach denen, die sich unauffällig verhalten, aber eben „anders“ sind – Fremde.

Was der Datenschutzbericht verrät:

„Bei der Datenverarbeitung in der Anti-Terror-Datei (ATD) habe ich einige Mängel festgestellt. Dies gilt insbesondere für die Problematik der Speicherung von ‚Randpersonen‘.“
Die so genannten Rand- oder Kontaktpersonen werden auch

als „Dolose“ bezeichnet. Man geht davon aus, dass sie von der Planung oder Begehung einer terroristischen Straftat oder der Ausübung, Unterstützung oder Vorbereitung von rechtswidriger Gewalt im Sinne des ATDG Kenntnis haben. Die Kontrolle des Bundesdatenschutzbeauftragten im März 2008 ergab unter anderem, dass es schwierig ist, „aussagefähige Belege oder tatsächliche Anhaltspunkte für eine belastbare Aussage zu einer entsprechend positiven Kenntnis zu eruieren“. Der Datenschutzbeauftragte schrieb: „Damit bestätigte sich meine Befürchtung, dass eine gesetzeskonforme Qualifizierung einer Kontaktperson als ‚dolos‘ auf der Grundlage objektiver Verhaltensumstände in der Praxis kaum möglich sein dürfte. Die hierfür herangezogenen Umstände und Erkenntnisse sind meist von vager oder ambivalenter Natur und rechtfertigen deshalb einen derartigen Eingriff in das Recht auf informationelle Selbstbestimmung des Einzelnen vielfach nicht.“ Im Klartext: Da werden jede Menge Daten über jede Menge Leute gespeichert, die weder auf gesicherten Erkenntnissen basieren noch einen tatsächlichen Verdacht rechtfertigen.

In einem Witz wird die einzig wirksame Maßnahme gegen staatliche Schnüffelwut im Zeichen der Terrorbekämpfung empfohlen: „Essen Sie Schweinefleisch und trinken Sie Alkohol. Nur so haben Sie eine Chance, sich nicht verdächtig zu machen.“ Politisch nicht korrekt und möglicherweise etwas übertrieben, aber vermutlich die einzige Empfehlung, die man mit einigermaßen Aussicht auf Erfolg geben kann.

Was der 11. September veränderte

Mit dem Anschlag auf das World Trade Center in New York am 11. September 2001 wurde eine neue Zeitrechnung in der Terrorbekämpfung und der staatlichen Datensammelwut eingeläutet. Der Kampf gegen die „Achse des Bösen“ und islamistische Selbstmordattentäter führte in einigen Staaten, allen voran die USA, dazu, dass die Freiheit gegenüber der Sicherheit in den Hintergrund trat. Im ersten Schock schossen die verantwortlichen Politiker teilweise übers Ziel hinaus. Im Zeichen der Terrorbekämpfung wurde so manches Gesetz auf den Weg gebracht oder geändert, dessen Wirksamkeit hinsichtlich der Terrorbekämpfung bezweifelt werden darf, aber dazu führt, dass jeder Bürger ins Ziel der Überwachungsgeräten, beispielhaft seien hier die Online-Durchsuchung und die zunehmende Videoüberwachung genannt. Die Gefahr besteht darin, zur falschen Zeit am falschen Ort zu sein, den falschen Namen zu tragen oder die falschen Freunde/Bekannteten zu haben.

Wer heute in die USA einreist und davor schon einmal in einem arabischen Land war, muss sich einen zweiten Reisepass ausstellen lassen, sonst läuft er Gefahr, nicht einreisen zu dürfen oder sich stundenlang Befragung durch die amerikanischen Sicherheitsbehörden auszusetzen. Vielen dürfte auch der Fall des Babys mit dem „falschen“ Namen im Gedächtnis geblieben sein. Die Passagiere eines Flugzeugs mit Ziel USA mussten stundenlang in der Maschine ausharren, weil ein Baby denselben Namen trug wie ein gesuchter Terrorist – es handelte sich übrigens um einen in der arabischen Welt so gebräuchlichen Namen wie bei uns Maier, Müller oder Schmidt.

In der Folge des 11. Septembers wurden in Deutschland eine ganze Reihe Gesetze und Vorschriften eingeführt, die das Ver-

halten von immer mehr Bürgern der staatlichen Beobachtung unterwerfen. Genannt seien hier:

- die Anti-Terror-Pakete der rot-grünen Bundesregierung („Otto-Kataloge“),
- das Terrorbekämpfungsergänzungsgesetz der Großen Koalition,
- die gemeinsame Anti-Terror-Datei von Polizeibehörden und Nachrichtendiensten,
- die Einführung biometrischer Merkmale in Reisepässen,
- die Kontendatenabfrage,
- weltweite Anti-Terror-Listen ohne jegliche Rechtsschutzmöglichkeit,
- die Vorratsdatenspeicherung (siehe dazu Kapitel 2).

Viele dieser neuen Instrumente werden zunehmend für andere Zwecke genutzt. Ein Beispiel ist die Kontendatenabfrage. Mittlerweile wird sie von Arbeitsagenturen, Finanzämtern und anderen Behörden zur Ermittlung der Einkommenssituation eingesetzt. Bedenklich ist zudem, dass der Staat nicht nur eigene Datensammlungen anlegt, sondern auch auf die aus der Privatwirtschaft zugreift. Bekanntestes Beispiel sind die Verkehrsdaten der Telekommunikation. Weniger bekannt ist, dass die Videoüberwachung oft nicht von Polizei oder anderen öffentlichen Stellen betrieben wird, sondern von Unternehmen und Privatleuten. Die Polizei bemüht sich darum, hier Zugriff zu erhalten. Jetzt mögen manche Zeitgenossen einwenden, wer nichts zu verbergen habe, brauche sich auch über die Videoüberwachung nicht aufzuregen. Mag sein, aber auch brave Bürger können ins Visier der Fahnder geraten. Man könnte als Kontakt- oder Begleitperson in irgendeine Datei geraten, zum Beispiel als Mitbewohner im Studentenwohnheim oder als Familienangehöriger eines Verdächtigen oder als Kollege.

Die Videoüberwachung ist übrigens auch ein Paradebeispiel für die Unsinnigkeit vieler Maßnahmen. In Großbritannien hat die Polizei selbst die Effektivität der Videokontrollen in Zweifel gezogen. Meistens sitze kein Polizeibeamter vor den Überwachungsmonitoren und auch für die Auswertung der gespeicherten Videoaufnahmen gebe es nicht genügend Personal. In London hätten die Videokameras deswegen keinerlei abschreckende Wirkung mehr. So weit, so gut. Allerdings hat die Polizei daraus nicht den Schluss gezogen, die Videoüberwachung aufzugeben, sondern fordert eine Nachrüstung der Technik, die ein automatisches Aufspüren verdächtigen Verhaltens und das Identifizieren der Personen ermöglicht.

In einem Vortrag in Chemnitz im Rahmen einer Veranstaltungsreihe des Bildungswerks Dresden der Konrad-Adenauer-Stiftung zum Thema „Anspruch auf Sicherheit und Frieden?“ sagte Peter Schaar, Bundesbeauftragter für den Datenschutz: „Bei vielen Maßnahmen und Regelungen stellt sich die Frage, ob die Grundrechtseingriffe im Hinblick auf den zu erwartenden Nutzen überhaupt **angemessen** sind. Wer neue Befugnisse für Strafverfolgung und Gefahrenabwehr fordert, muss begründen, warum er mit den bestehenden Befugnissen nicht auskommt. Leider läuft es in der Realität häufig umgekehrt: Diejenigen, die für Freiheitsrechte eintreten und Grundrechte verteidigen, haben sich zu rechtfertigen.“

Was uns die Terrorismusbekämpfungsgesetze bringen:

- Rasterfahndung
- Sicherheitsüberprüfung
- Verfassungsschutzanfragen
- Späh- und Lauschangriffe

- Videoüberwachung
- Telekommunikationsüberwachung
- Finanzkontrolle
- Ausländerüberwachung
- Biometrische Ausweise

Vom „Otto-Katalog“ zum Terrorcamp-Gesetz

Mit dem **Gesetz zur Bekämpfung des internationalen Terrorismus** vom 9. Januar 2002, nach dem damaligen Innenminister Otto Schily auch als „Otto-Katalog“ bekannt, begann der Staat damit, eine ganze Reihe von Grundrechten auszuhöhlen. Darin enthalten waren Änderungen des Bundesverfassungsschutz- und des BND-Gesetzes, die dem Verfassungsschutz und dem Bundesnachrichtendienst weit reichende neue Befugnisse zuerkannten. Auch das Geldwäschegesetz, das Sicherheitsüberprüfungsgesetz, die Gesetze über Pässe und Personalausweise, das Bundesgrenzschutz- und das Bundeskriminalamtgesetz, das Vereins- und das Ausländergesetz, das Asylverfahrensgesetz und das Gesetz über das Ausländerzentralregister wurden in diesem Rahmen geändert. Eine Reihe dazugehöriger Verordnungen wurde ebenfalls überarbeitet. Änderungen erfuhr auch das Luftverkehrs- und das Bundeszentralregister- sowie das Energiesicherheitsgesetz. Selbst vor dem Sozialgesetzbuch machte die Änderungswut der Politik keinen Halt. Viele der Änderungen beziehen sich auf das Ausspionieren von Telekommunikationsdaten und die Weitergabe von Daten an andere Behörden. Für den Bürger ist die Vielzahl der kleinen Änderungen so gut wie nicht nachvollziehbar. Vor allem ist es schwierig zu erkennen, welche Folgen die Änderungen in letzter Konsequenz haben.

Thilo Weichert, damals Vorsitzender der Deutschen Vereinigung für Datenschutz (DVD) zog im September 2002 eine erste Bilanz. Nach seiner Meinung hatten die neuen Gesetze „nichts Nachweisbares zur Aufklärung terroristischer Straftaten beigetragen und sind hierzu nicht geeignet“. Die Erfolge der Ermittlungsbehörden beruhten auf „klassischer, schon bisher zulässiger kriminalistischer Arbeit“. Die 2002 durchgeführte bundesweite Rasterfahndung nach so genannten Schläfern war laut Weichert „ein gewaltiger, finanziell und personell aufwändiger ‚Schlag ins Wasser‘“. Und auch die „massiv verschärfte Ausländerüberwachung“ habe nur eine Verunsicherung und Verängstigung der Betroffenen bewirkt. Zu den weiteren Absichten des Gesetzgebers sagte Weichert: „Hochgradig beängstigend ist, dass Politiker fast jeder Couleur im Schatten des 11. Septembers solche Maßnahmen beschlossen haben und weiter vorantreiben, oft ohne über die Gefahren zum Beispiel für den Datenschutz auch nur nachzudenken. Es wäre ein später fataler Sieg der Terroristen, wenn unser Rechtsstaat unter dem Vorwand von deren Bekämpfung sich aufgäbe.“ Er forderte weiter eine „wissenschaftliche Bewertung der bisherigen Kompetenzen, die Feststellung der grundrechtlichen Auswirkungen und die Beschneidung des ineffektiven und unverhältnismäßigen Wildwuchses an Ermittlungsbefugnissen“.

Doch die Politiker ließen sich nicht beirren und schoben im Laufe der Jahre weitere Gesetze nach. Einige seien hier genannt. Als Erstes wurde die Gültigkeit der Anti-Terror-Gesetze 2007 um weitere fünf Jahre verlängert. Ende 2008 passierte das neue **BKA-Gesetz** den Bundestag, über das wir Sie ausführlich im nächsten Kapitel informieren. Dabei wurden trotz Protesten von Datenschützern weder der große Lausch- und Spähangriff noch die Online-Durchsuchung und die Rasterfahndung gestrichen. In über 20 komplizierten Paragraphen erhält das BKA zum Beispiel das Recht, Journalisten, Ärzte und Rechtsanwälte zu

überwachen, heimlich in deren Wohnungen einzudringen und private Computer zu manipulieren. Die vom BKA gewonnenen Daten dürfen danach sogar noch zur Verfolgung weiterer Straftaten verwendet werden, die gar nicht mit terroristischen oder schweren Straftaten zu tun haben müssen.

Der Datenschutzbeauftragte zum BKA-Gesetz:

„Die dem BKA eingeräumten heimlichen Eingriffsbefugnisse greifen in einer Weise in die Persönlichkeitsrechte ein, die bislang ganz wesentlich den Nachrichtendiensten vorbehalten waren. Waren bei den Nachrichtendiensten die so genannten nachrichtendienstlichen Mittel deshalb vertretbar, weil die Dienste keinerlei exekutive Befugnisse besitzen, so verhält sich dies hier anders: Wenden Polizeibehörden heimliche Ermittlungsmethoden an, können diese mit exekutiven Befugnissen verbunden werden. Dies erhöht die Eingriffintensität und die Folgen für den Betroffenen ganz erheblich.“

Kein bisschen besser ist das so genannte **Terrorcamp-Gesetz**, das jüngste der Terrorbekämpfungsgesetze. Damit sollen terroristische Straftaten im Vorfeld verhindert werden. Zum ersten Mal besteht in Deutschland die Möglichkeit, schon für die Vorbereitung von Gewalttaten oder die Verbreitung von Anleitungen dazu bestraft zu werden. Das ist eine neue Qualität in der Gesetzgebung. Jens Puschke, Vorstandsmitglied der Bürgerrechtsorganisation „Humanistische Union“, weist auf die unübersehbaren Folgen hin: „Nach dem Gesetz soll beispielsweise die Aneignung von Fertigkeiten bestraft werden, die später möglicherweise für die Ausübung einer Gewalttat nutzbar sind. Der Gesetzestext ist dabei allerdings so unbestimmt, dass beispielsweise auch das Erlernen einer Sprache darunter fallen würde, schließlich könnten

die Täter in der Vorbereitung ihrer Anschläge miteinander kommunizieren.“ Der Einwand Puschkes macht deutlich, worum es geht: die Auslegung. Bundesjustizministerin Brigitte Zypries versicherte zwar, dass es sich um die Vorbereitung schwerer staatsgefährdender Straftaten handeln müsse, damit das Gesetz greife, andererseits lässt sich natürlich nicht leugnen, dass mit der so genannten Vorfeldstrafbarkeit eine neue Dimension erreicht wird. Jemanden für mögliche Absichten zu bestrafen ist zweifelhaft. Strafrecht darf kein Gefahrenbekämpfungsrecht sein.

Möchten Sie weiterlesen? Unser Buch erhalten Sie bei Ihrem Buchhändler oder im Webshop des Mankau Verlags: www.mankau-verlag.de.